

FILED
U.S. DISTRICT COURT
DISTRICT OF MARYLAND

2019 MAY 14 AM 11:58

CLERK'S OFFICE
AT GREENBELT

BY KM DEPUTY

WD EGW/KOH: USAO 2018R00264

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

TARE STANLEY OKIRIKA,

Defendant

CRIMINAL NO. GJH 19CR048

(Conspiracy to Commit Wire Fraud,
18 U.S.C. § 1349; Forfeiture, 18 U.S.C.
§ 981(a)(1)(C), 21 U.S.C. § 853(p),
28 U.S.C. § 2461(c))

INFORMATION

COUNT ONE
(Conspiracy to Commit Wire Fraud)

The United States Attorney for the District of Maryland charges that:

Introduction and Background

At all times relevant to this Information:

1. Defendant TARE STANLEY OKIRIKA (“OKIRIKA”) was a resident of Maryland.
2. Co-conspirator 1 was a resident of Maryland.
3. Co-conspirator 2 was a resident of Nigeria.
4. The Federal Emergency Management Agency (“FEMA”) was an agency of the United States, within the United States Department of Homeland Security (“DHS”), responsible for providing emergency benefits and compensation for damage to victims who were affected by declared national emergency disasters. Among other benefits, an individual in an area affected by a national disaster was immediately eligible for \$500 in compensation, deemed “Critical Needs Assistance” (“CNA”), for the purpose of enabling the purchase of life-saving or life-

sustaining materials. The assistance was provided in the form of funds with no spending limitations and was paid to the victim in a manner of his/her choosing, among available options, which could include being paid onto pre-paid debit cards. The servers for FEMA, which were used for processing applications for assistance, were located in Kansas City, Missouri, and Mount Weather, Virginia.

5. The Social Security Administration (“SSA”) was an agency of the United States responsible for paying Social Security benefits to, for example, individuals who had met their retirement age and were entitled to retirement benefits. The benefits were paid to each beneficiary in a manner of his/her choosing, among available options, which could include being paid onto pre-paid debit cards.

6. The U.S. Department of Labor, working with its associated entities (“DOL”), was an agency of the United States responsible for administering unemployment and disability compensation benefits to eligible workers. The benefits were paid to the beneficiary in a manner of his/her choosing, among available options, which could include being paid onto pre-paid debit cards.

7. The Internal Revenue Service (“IRS”) was an agency of the United States responsible for administering the country’s internal revenue laws. If individuals submitted materials indicating that they had paid taxes to the IRS that were determined to exceed the tax liability due and owing, then the individuals would be entitled to refunds of that tax. The refunds were paid to the individual in a manner of his/her choosing, among available options, which could include being paid onto pre-paid debit cards.

8. Green Dot pre-paid debit cards were pre-paid debit cards that could be purchased at convenience, pharmacy, and grocery stores nationwide and, upon registration, could be funded by Automated Clearing House (“ACH”) electronic funds transfers in the same manner as a bank account. Green Dot’s headquarters, to which electronic communications traveled in connection with each Green Dot debit card transaction, including to have money deposited onto the card, were located in Pasadena, California.

9. Each Green Dot pre-paid debit card had a unique number and had to be loaded with an initial dollar amount by the card purchaser, usually \$10 or \$20 cash. An individual could then register the card online at GreenDot.com, including from a mobile phone. For registration, individuals were able to use any real individual’s name and address.

10. Upon registration of a Green Dot card, Green Dot issued an account number and provided a routing number for Green Dot Bank. Although Green Dot undertook efforts to confirm that the identifying information provided upon registration of a card matched a real person, a Green Dot card, unlike most bank-issued credit and debit cards, did not require that an activation code or Personal Identification Number (“PIN”) be mailed to the registered cardholder. Rather, each card was sold with a PIN that could be used to withdraw funds from ATMs or otherwise fund purchases in the manner of a debit card. Individuals could also subsequently amend the card’s PIN.

11. An individual could put money onto Green Dot debit cards in a variety of manners, including by way of cash or electronically from bank accounts, government agencies, or other sources.

12. For Green Dot debit cards, users were able, if the cards were registered with Green Dot, to log into an online account portal or a mobile application to control funds, as well as to utilize the debit card for purchases and withdrawals.

13. WhatsApp was an encrypted Internet-based multimedia messaging service used via a smartphone application that functioned using both cellular and wireless data connections.

The Conspiracy

14. From a time unknown to the United States Attorney, but beginning at least in or about June 2017, and continuing through at least in or about August 2018, in the District of Maryland and elsewhere, the defendant,

TARE STANLEY OKIRIKA,

did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to commit wire fraud, that is, to devise any scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises (“the scheme to defraud”), and for the purpose of executing and attempting to execute such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, any writings, signs, signals, pictures, and sounds, in violation of 18 U.S.C. § 1343, in relation to, and involving any benefit authorized, transported, transmitted, transferred, disbursed, and paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. § 5122)).

Manner and Means of the Conspiracy and Scheme to Defraud

It was part of the conspiracy and scheme to defraud that:

15. In and around 2016 and 2017, **OKIRIKA**, Co-conspirator 1, and other co-conspirators purchased hundreds of Green Dot debit cards at convenience stores, pharmacies, and grocery stores. Co-conspirators then registered those cards with Green Dot using stolen personally identifiable information (“PII”) of victims of identity theft from around the country.

16. Amidst Hurricanes Harvey, Irma, and Maria, and the California wildfires in 2017, which were presidentially declared major disasters or emergencies, the co-conspirators applied online with FEMA for CNA using the stolen PII of additional victims of identity theft, who were eligible for \$500 due to those disasters. FEMA paid at least approximately \$8 million in amounts of \$500 per claim to the Green Dot debit cards, among other pre-paid debit cards, purchased by the co-conspirators.

17. In addition to filing false disaster assistance claims with FEMA, co-conspirators also filed online false claims for Social Security benefits, false claims for IRS tax refunds, and false claims for DOL unemployment and disability benefits using the stolen identities of multiple additional individuals, including name, address, Social Security Number (“SSN”), and other personal identifiers.

18. When filing the claims online, co-conspirators input the account number and routing number from the Green Dot debit card into the claim form in order to receive the disaster assistance or other government program funds such as Social Security benefits, IRS tax refunds, and DOL benefits, on the Green Dot debit card.

19. By virtue of the applications, the federal agencies to whom the applications had been submitted then ACH-deposited claims proceeds directly onto the Green Dot debit cards. Funds were deposited onto the Green Dot debit cards in multiple stolen identities, and in stolen identities that were different from the identities that had been used to register the cards.

20. After the funds were placed onto the Green Dot debit cards, the co-conspirators, including Co-conspirator 2, informed **OKIRIKA** and others, such as Co-conspirator 1, that funds were available on the cards, and provided information to those co-conspirators to facilitate “cashing out” the funds from the cards, which those and other co-conspirators did in exchange for a commission.

21. **OKIRIKA**, Co-conspirator 1, and other co-conspirators subsequently spent, deposited into bank accounts, and/or “cashed out,” through ATM withdrawals or the purchase of money orders, for instance, the funds placed on the pre-paid debit cards, in the District of Maryland and elsewhere. The co-conspirators regularly “cashed out” from cards soon after funds were added to a card.

22. **OKIRIKA**, Co-conspirator 1, and other co-conspirators took steps to conceal their identities and the conspiracy and scheme to defraud, such as by enlisting other individuals to make purchases and withdrawals, utilizing multiple different store and bank locations and methods of withdrawal, using multiple different bank accounts (including in the names of corporate entities) and banks, converting funds into cash rather than placing them into bank accounts, and making money orders payable to other individuals and/or corporate entities which they or their co-conspirators controlled.

23. **OKIRIKA** defrauded the United States and obtained money from the United States both by receiving such funds himself and by directing Co-conspirator 1 to "cash out" stolen funds from Green Dot and other pre-paid debit cards, onto which co-conspirators had loaded those stolen funds.

24. **OKIRIKA**, Co-conspirator 1, Co-conspirator 2, and other co-conspirators communicated by way of WhatsApp, e-mail, and other methods in furtherance of the scheme.

25. **OKIRIKA** used stolen federal funds from the scheme to pay his rent, to purchase used vehicles, and for other purposes.

18 U.S.C. § 1349

FORFEITURE ALLEGATION

The United States Attorney for the District of Maryland further finds that:

1. Pursuant to Fed. R. Crim. P. 32.2, notice is hereby given to the defendant that the United States will seek forfeiture as part of any sentence in accordance with 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), in the event of the defendant's conviction on Count One of this Information.

Fraud Forfeiture

2. As a result of the offense set forth in Count One, the defendant,

TARE STANLEY OKIRIKA,

shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such violation, and all interest and proceeds traceable thereto, including but not limited to at least \$51,839.44 in United States currency.

Substitute Assets

3. If, as a result of any act or omission of any defendant, any of the property described above as being subject to forfeiture:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or,
- e. has been commingled with other property which cannot be subdivided without difficulty,

the United States of America, pursuant to 21 U.S.C. § 853(p), shall be entitled to forfeiture of substitute property.

18 U.S.C. § 981(a)(1)(C)
21 U.S.C. § 853(p)
28 U.S.C. § 2461(c)

Date: May 14, 2019

Robert K. Hur^{b7Ew}
Robert K. Hur
United States Attorney